

A solution of an equivalence problem for semisimple cyclic codes

Mikhail Muzychuk

ABSTRACT. In this paper we propose an efficient solution of an equivalence problem for semisimple cyclic codes.

1. Introduction

Recall that an $[n, k]_q$ code is a k -dimensional subspace \mathcal{C} of \mathbb{F}_q^n . Two $[n, k]_q$ codes $\mathcal{C}, \mathcal{D} \leq \mathbb{F}_q^n$ are called (*permutation*) *equivalent*, notation $\mathcal{C} \sim \mathcal{D}$, if one of them may be obtained from another one by permuting the coordinates. A linear code is called *cyclic* if it is invariant under a cyclic shift of the coordinates. An equivalence problem for cyclic codes, and, more generally, an isomorphism problem for arbitrary cyclic objects, was studied by many authors during last three decades [1, 16, 8, 17, 2, 6, 4, 11, 3, 14] - to mention a few. In the paper [6] Huffman, Job and Pless completely solved an isomorphism problem for arbitrary cyclic combinatorial objects on p^2 points where p is a prime. The solution was given in terms of *generalized multipliers* and was generalized in [15] via a notion of a *solving set*: a set of permutations S is called a solving set for a class of cyclic objects when two cyclic objects from the class are equivalent if and only if they are equivalent by a permutation from S . It was shown in [15] that there exists a solving set for colored circulant digraphs of order n of cardinality $O(n^2 \varphi(n))$. Moreover this set may be efficiently constructed from n without any additional information. The main result of this paper states that a solving set constructed in [15] is also good for cyclic semisimple codes. To formulate precise results we need more definitions.

Each cyclic code of length n over finite field \mathbb{F}_q may be considered as an ideal in the group algebra $\mathbb{F}_q[H]$ of a cyclic group H of order n . Notice that if H is an arbitrary group, then a *group code* is an arbitrary right ideal of $\mathbb{F}_q[H]$. In what follows we write $I \trianglelefteq \mathbb{F}_q[H]$ to designate the fact that I is a right ideal of $\mathbb{F}_q[H]$. A group code $I \trianglelefteq \mathbb{F}_q[H]$ is called *semisimple* if the group algebra $\mathbb{F}_q[H]$ is semisimple, that is $\gcd(q, |H|) = 1$. An automorphism group of a group code always contains a subgroup H_R consisting of right translations by the elements of H . This group acts regularly on the coordinates of a group code. Thus a group code is a particular case of a *Cayley combinatorial object* introduced by L.Babai [1]. Recall that a Cayley combinatorial object over a group H is any relational structure on H invariant under the group H_R . Let \mathcal{K} be a class of Cayley combinatorial objects over the group H . Two objects from \mathcal{K} are called *Cayley isomorphic* if there exists an automorphism H which maps one of them onto another. An object $K \in \mathcal{K}$ is called a *CI-object* if any $K' \in \mathcal{K}$ isomorphic to K is also Cayley isomorphic to K . A group H is called a *CI-group* with respect to the class

\mathcal{K} if any object $K \in \mathcal{K}$ is a CI-object. Two classes of Cayley objects are essential for this paper: group codes and *colored Cayley digraphs*.

A colored Cayley digraph over a finite group H is a pair (H, ϕ) where $\phi : H \rightarrow C$ is a function to the set of colors C . An arc $(x, y) \in H \times H$ is colored by a color $\phi_{xy^{-1}}$. We denote the corresponding colored Cayley digraph as $\text{Cay}(H, \phi)$. An isomorphism between two colored Cayley digraphs is defined in a natural way (see the next section where all related definitions are given). In the case when a coloring set C is a finite field we identify the coloring function $\phi : H \rightarrow \mathbb{F}_q$ with an element of a group algebra $\sum_{h \in H} \phi(h)h$.

Now we are able to formulate the main result of the paper.

Theorem 1. *Let H be a cyclic group of order n written multiplicatively. Let $I \trianglelefteq \mathbb{F}_q[H]$ be a semisimple cyclic code over H generated by the idempotent $e = \sum_{h \in H} e_h h \in \mathbb{F}_q[H]$. Then a solving set for $\text{Cay}(H, e)$ is a solving set for I .*

It was shown in [15] that a solving set S_e for a given colored Cayley digraph $\text{Cay}(\mathbb{Z}_n, e)$ over a cyclic group of order n contains at most $\varphi(n)$ permutations. This set depends only on a partition \mathcal{P}_e of H constructed from the coloring e in the following way: two elements $a, b \in H$ belong to the same class of \mathcal{P}_e whenever $e_a = e_b$. Once a partition \mathcal{P}_e is built, a construction of the related solving set requires $O(n^2)$ arithmetic operations in the ring \mathbb{Z}_n . When the set S_e is produced an equivalence testing becomes rather simple: a cyclic code $J \trianglelefteq \mathbb{F}_q[H]$ is equivalent to the code $I = e\mathbb{F}_q[H]$ if and only if it is equivalent by a permutation from S_e . This gives a simple algorithm for a code equivalence testing which is polynomial in n and q .

It was shown in [12] [13] that a cyclic group of a square-free or twice square free order is a CI-group with respect to colored Cayley digraphs. In this case Theorem 1 implies the following

Theorem 2. *A cyclic group of a square-free or twice square-free order is a CI-group with respect to semisimple cyclic codes.*

The proof of Theorem 1 is based on the results of [14] which were obtained using the classification of finite simple groups (CFSG). It would be nice to find a classification-free proof of this result. Notice that if n is a prime power, then the CFSG is not needed. Also for non-cyclic p -groups we have additional results.

Theorem 3. *Let H be a p -group, p a prime. Then any solving set for colored Cayley digraphs over H is a solving set for semisimple group codes over H . In particular, if H is a CI-group with respect to colored Cayley digraphs, then it is a CI-group with respect to semisimple codes.*

It was shown in [5] that an elementary abelian group of rank at most four is a CI-group with respect to colored digraphs. This implies the following

Corollary 1. *An elementary abelian group of rank at most four is a CI-group with respect to semisimple group codes over this group.*

Notation. Throughout the paper Ω denotes a finite set and \mathbb{F}_q stands for a finite field with q elements. The set of all functions from Ω to \mathbb{F}_q is denoted as \mathbb{F}_q^Ω . The elements of \mathbb{F}_q^Ω are considered either as functions or column vectors the coordinate positions of which are labelled by the elements of Ω . For $f \in \mathbb{F}_q^\Omega$ we denote the ω -th coordinate of f either by $f(\omega)$ or f_ω . The algebra $\text{End}(\mathbb{F}_q^\Omega)$ is identified with the matrix algebra $M_\Omega(\mathbb{F}_q)$. The symmetric group of the set Ω is denoted by $\text{Sym}(\Omega)$. Given a permutation $g \in \text{Sym}(\Omega)$, we write P_g for a permutation matrix corresponding to g . Notice that $P_g \in M_\Omega(\mathbb{F}_q)$.

2. Preliminaries

2.1. Linear codes. In order to treat linear codes as combinatorial objects over finite set Ω we consider codes as linear subspaces of \mathbb{F}_q^Ω . If $g \in \text{Sym}(\Omega)$, then $f^g(\omega) := f(\omega^{g^{-1}})$. Recall that two codes $\mathcal{C}, \mathcal{D} \leq \mathbb{F}_q^\Omega$ are (permutation) equivalent if there exists $g \in \text{Sym}(\Omega)$ with $\mathcal{C}^g = \mathcal{D}$. An *automorphism* group of a code \mathcal{C} , notation $\text{PAut}(\mathcal{C})$, consists of those $g \in \text{Sym}(\Omega)$ which satisfy $\mathcal{C}^g = \mathcal{C}$. A code \mathcal{C} is called cyclic if $\text{PAut}(\mathcal{C})$ contains a full cycle.

2.2. Colored digraphs. Let Ω and F be finite sets. An F -colored digraph is a pair $\Gamma = (\Omega, c)$ where c is a function $c : \Omega \times \Omega \rightarrow F$. An adjacency matrix of Γ , $A(\Gamma) \in M_\Omega(F)$, is defined in a natural way $A(\Gamma)_{\omega, \omega'} = c(\omega, \omega')$. Two F -colored graphs (Ω, c) and (Ω, d) are isomorphic if there exists a permutation $g \in \text{Sym}(\Omega)$ such that $d(\alpha^g, \beta^g) = c(\alpha, \beta)$ for each pair $\alpha, \beta \in \Omega$. An automorphism group $\text{Aut}(\Gamma)$ consists of all isomorphisms from Γ to itself, that is

$$g \in \text{Aut}(\Gamma) \iff \forall_{\alpha, \beta \in \Omega} c(\alpha, \beta) = c(\alpha^g, \beta^g).$$

If F is a field, then $\text{Aut}(\Gamma)$ consists of all permutations $g \in \text{Sym}(\Omega)$ satisfying $P_g A(\Gamma) = A(\Gamma) P_g$. Thus $\text{Aut}(\Gamma)$ coincides with the centralizer of $A(\Gamma)$ in $\text{Sym}(\Omega)$, i.e., $\text{Aut}(\Gamma) = \mathbf{C}_{\text{Sym}(\Omega)}(A(\Gamma))$.

Let H be a finite group and F an arbitrary field. Recall that a colored Cayley digraph $\text{Cay}(H, e)$ defined by an element $e = \sum_{h \in H} e_h h \in F[H]$ has H as a vertex set and an arc-coloring is defined by a function $(x, y) \mapsto e_{xy^{-1}}, x, y \in H$. Its adjacency matrix will be denoted as $A_H(e)$. Clearly that $(A_H(e))_{xy} = e_{xy^{-1}}$. The set of all matrices $A_H(e), e \in F[H]$ form a subalgebra of the full matrix algebra $M_H(F)$. This subalgebra is isomorphic to the group algebra $F[H]$. Let us call matrices of the form $A_H(e)$ as H -matrices. Each H -matrix commutes with any permutation from H_R . Vice versa, any matrix from $M_H(F)$ which commutes with all permutations from H_R is an H -matrix. Thus the algebra of H -matrices is the centralizer of H_R in the full matrix algebra $M_H(F)$.

2.3. 2-closed permutation groups [19]. Any subgroup $G \leq \text{Sym}(\Omega)$ acts naturally on a product $\Omega \times \Omega$ as follows $(\alpha, \beta)^g := (\alpha^g, \beta^g)$. The orbits of this faithful action are called *2-orbits* of G . The set of all 2-orbits will be denoted as Ω^2/G . Two subgroups $G, F \leq \text{Sym}(\Omega)$ are called *2-equivalent*, notation $G \sim_2 F$ if $\Omega^2/G = \Omega^2/F$. The relation \sim_2 is an equivalence relation on the set of all subgroups of $\text{Sym}(\Omega)$. For a given subgroup $G \leq \text{Sym}(\Omega)$ we define its 2-closure $G^{(2)}$ as the subgroup generated by all subgroups 2-equivalent to G , that is

$$G^{(2)} := \langle F \mid F \sim_2 G \rangle.$$

Notice that $G \sim_2 G^{(2)}$ and $G^{(2)} = F^{(2)}$ if and only if $G \sim_2 F$. The operator $G \mapsto G^{(2)}$ satisfies the usual properties of a closure operator. Notice that an intersection of two 2-closed groups is also 2-closed. The connection between colored digraphs and 2-closed permutation groups is given in the statement below which is a direct consequence of Theorem 5.23 [19] (see also Section 7.12 in [9])

Theorem 4. *An automorphism group of a colored digraph is 2-closed. Vice versa, any 2-closed permutation group is an automorphism group of a colored digraph.*

Each matrix $A \in M_\Omega(\mathbb{F}_q)$ is an adjacency matrix of an \mathbb{F}_q -colored digraph with vertex set Ω . Therefore $\mathbf{C}_{\text{Sym}(\Omega)}(A)$ is a 2-closed subgroup of $\text{Sym}(\Omega)$.

3. Proof of main results

Let $\mathcal{C} \leq \mathbb{F}_q^\Omega$ be a linear code. A *projector* onto \mathcal{C} is an endomorphism $E \in M_\Omega(\mathbb{F}_q)$ such that $E^2 = E$ and $\text{Im}(E) = \mathcal{C}$. The latter condition is equivalent to saying that the column space of E coincides with \mathcal{C} . Clearly that $\text{Im}(E) \oplus \text{Ker}(E) = \mathbb{F}_q^\Omega$. Notice that each projector onto \mathcal{C} is uniquely determined by its kernel which is a subspace complementary to \mathcal{C} . Given a subspace \mathcal{C}' complementary to \mathcal{C} in \mathbb{F}_q^Ω , one can define a projector E onto \mathcal{C} by setting $Ev = v$ for $v \in \mathcal{C}$ and $Ev = 0$ for $v \in \mathcal{C}'$. So there is a one-to-one correspondence between projectors onto \mathcal{C} and complements to \mathcal{C} in \mathbb{F}_q^Ω . If a permutation matrix $P_g, g \in \text{Sym}(\Omega)$ commutes with E , then $\mathcal{C}^g = \mathcal{C}$. This implies the following

Proposition 1. *Let E be a projector onto a code \mathcal{C} . Then $\mathbf{C}_{\text{Sym}(\Omega)}(E) \leq \text{PAut}(\mathcal{C})$.*

Theorem 5. *Let $G \leq \text{PAut}(\mathcal{C})$ be a subgroup of order coprime to q . Then $G^{(2)} \leq \text{PAut}(\mathcal{C})$.*

PROOF. The group algebra $\mathbb{F}_q[G]$ is semisimple by Maschke's Theorem. Therefore each $\mathbb{F}_q[G]$ -module is semisimple too. This implies that each G -invariant subspace of \mathbb{F}_q^Ω has a G -invariant complement. Therefore there exists a G -invariant complement \mathcal{C}' to \mathcal{C} in \mathbb{F}_q^Ω . Let E denote a projector on \mathcal{C} with a kernel \mathcal{C}' . Then E commutes with each $P_g, g \in G$, or, equivalently, $G \leq \mathbf{C}_{\text{Sym}(\Omega)}(E) \leq \text{PAut}(\mathcal{C})$. Since $\mathbf{C}_{\text{Sym}(\Omega)}(E)$ is 2-closed, $G^{(2)} \leq \mathbf{C}_{\text{Sym}(\Omega)}(E) \leq \text{PAut}(\mathcal{C})$. ■

By Exercise 5.28 [19] a 2-closure of a p -group is a p -group. This gives us the following

Corollary 2. *Each Sylow r -subgroup of $\text{PAut}(\mathcal{C})$, $r \neq \text{char}(\mathbb{F}_q)$ is 2-closed.*

3.1. Fusion control. Let $X \leq Y \leq Z \leq \text{Sym}(\Omega)$ be arbitrary subgroups. Following [10] we say that Y *controls fusion of X in Z* if for any $g \in \text{Sym}(\Omega)$ the following implication holds

$$X^g \leq Z \implies \exists_{z \in Z} X^{gz} \leq Y.$$

In this case we write $Y \prec_X Z$. If X is a regular subgroup of $\text{Sym}(\Omega)$, then the inequality $Y \prec_X Z$ means that for any regular subgroup $X' \leq Z$ isomorphic to X there exists $z \in Z$ such that $X'^z \leq Y$.

The following properties of the relation \prec_X are straightforward:

- (a) \prec_X is a transitive relation on a set of all overgroup of X in $\text{Sym}(\Omega)$;
- (b) if $Y \prec_X Z$ and $Y \leq W \leq Z$, then $W \prec_X Z$.

The statement below is a direct generalization of Lemma 3.1 from [1].

Theorem 6. *Let K, L be two Cayley objects over H . If $\text{Aut}(K) \prec_{H_R} \text{Aut}(L)$, then each solving set for K is a solving set for L . In particular, if K is a CI-object over H , then so does L .*

PROOF. Let S be a solving set for K . Pick an arbitrary Cayley object over H , say L' isomorphic to L . Then $L' = L^g$ for some $g \in \text{Sym}(\Omega)$ and, consequently, $\text{Aut}(L') = \text{Aut}(L)^g$. Therefore $H_R \leq \text{Aut}(L)^g$ implying $H_R^{g^{-1}} \leq \text{Aut}(L)$. By the assumption there exists $z \in \text{Aut}(L)$ such that $H_R^{g^{-1}z^{-1}} \leq \text{Aut}(K)$. This implies that $H_R \leq \text{Aut}(K)^{zg} = \text{Aut}(K^{zg})$. Thus K^{zg} is a Cayley object over H isomorphic to K . Therefore $K^{zg} = K^s$ for some $s \in S$. Since $zgs^{-1} \in \text{Aut}(K) \leq \text{Aut}(L)$, we conclude that $L^{zgs^{-1}} = L$, or, equivalently, $L^{zg} = L^s$. Together with $z \in \text{Aut}(L)$ and $L^g = L'$ we obtain $L' = L^s$. ■

PROOF OF THEOREM 3. Let P be a Sylow p -subgroup of $\text{PAut}(I)$ containing H_R . By Sylow's theorems $P \prec_{H_R} \text{PAut}(I)$.

Since $\mathbb{F}_q[P]$ is semisimple, there exists an $\mathbb{F}_q[P]$ -invariant complement to I in $\mathbb{F}_q[H]$, say J . Let E be a projection on I parallel to J . Since E commutes with all permutations from P , it also commutes with H_R . Therefore E is an H -matrix, that is $E = A_H(e)$ for some $e \in \mathbb{F}_q[H]$. It follows from $\text{Im}(E) = I$ that $e\mathbb{F}_q[H] = I$. An equality $E^2 = E$ implies that e is an idempotent. Since P centralizes $A_H(e)$ and $\mathbf{C}_{\text{Sym}(H)}(A_H(e)) \leq \text{PAut}(I)$, we obtain $P \leq \mathbf{C}_{\text{Sym}(H)}(A_H(e)) \leq \text{PAut}(I)$. Therefore $\mathbf{C}_{\text{Sym}(H)}(A_H(e)) \prec_{H_R} \text{PAut}(I)$. Since $A_H(e)$ is the adjacency matrix of a colored Cayley graph $\text{Cay}(H, e)$, we conclude that $\mathbf{C}_{\text{Sym}(H)}(A_H(e)) = \text{Aut}(\text{Cay}(H, e))$. By Theorem 6 any solving set for a colored Cayley graph $\text{Cay}(H, e)$ is a solving set for a code I . ■

Notice that if H is commutative, then an idempotent e is unique. In the case of non-commutative H a right ideal of $\mathbb{F}_q[H]$ may have more than one generating idempotent.

PROOF OF THEOREM 1. By Theorem 1.8 [14] there exists a solvable group F , $H_R \leq F \leq \text{PAut}(I)$ which controls fusion of H_R in $\text{PAut}(I)$. Let π be the set of all prime divisors of n . It follows from Hall's theorems that every Hall π -subgroup $F_\pi \leq F$ which contains H_R controls fusion of H_R in F . By transitivity of \prec_{H_R} the group F_π controls fusion of H_R in $\text{PAut}(I)$. Since $\text{char}(\mathbb{F}_q)$ is coprime to $|F_\pi|$, there exists a F_π -invariant complement J to I in $\mathbb{F}_q[H]$. Let E denote a projector onto I parallel to J . Then $F_\pi \leq \mathbf{C}_{\text{Sym}(H)}(E) \leq \text{PAut}(I)$ implying $\mathbf{C}_{\text{Sym}(H)}(E) \prec_{H_R} \text{PAut}(I)$. Since $H_R \leq \mathbf{C}_{\text{Sym}(H)}(E)$, the matrix E is circulant, that is $E = A_H(e)$ for some $e \in \mathbb{F}_q[H]$. It follows from $E^2 = E$ and $\text{Im}(E) = I$ that e is an idempotent generating I . Thus $\mathbf{C}_{\text{Sym}(H)}(A_H(e)) = \text{Aut}(\text{Cay}(H, e))$ controls fusion of H_R in $\text{PAut}(I)$. By Theorem 6 any solving set for $\text{Cay}(H, e)$ is a solving set for I . ■

4. Acknowledgements

The author is very grateful to I. Ponomarenko and M. Klin for fruitful discussions and valuable remarks.

References

- [1] L. Babai, *Isomorphism problem for a class of point-symmetric structures*, Acta Math. Acad. Sci. Hungar. **29**(1977), 329-336.
- [2] N. Brand, *Isomorphisms of cyclic combinatorial objects*, Discrete Math. **78** (1989), no. 1-2, 7381.
- [3] E. Dobson, *On the Cayley isomorphism problem*, Discrete Mathematics **247** (2002), 107116.
- [4] S.Evdokimov and I.Ponomarenko. *Circulant graphs: recognizing and isomorphism testing in polynomial time*, St. Petersburg Math. J., Vol. 15 (2004), No. 6, 813835.
- [5] M. Hirasaka, M. Muzychuk, *The elementary abelian group of rank 4 is a CI-group*, J. of Combin. Theory (A), **94**, 339-362 (2001) .
- [6] W.G. Huffman, A. Job, V. Pless, *Multipliers and generalized multipliers of cyclic objects and cyclic codes*, J. of Comb. Th. (A) **62**(1993), no. 2, 183-215.
- [7] W.C. Huffman, *The equivalence of two cyclic objects on pq elements*, Discrete Math. **154**(1996), 103-127.
- [8] M.H. Klin, R. Pöschel, *The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings*, Colloq. Math. Soc. J. Bolyai **25**, Algebraic methods in graph theory, Szeged, 1978. North-Holland, Amsterdam, 1981; 405-434.
- [9] M. Klin, C. Rückert, G. Rückert, G. Tinhofer. Algebraic Combinatorics in Mathematical Chemistry. Methods and Algorithms. I. Permutation Groups and Coherent (Cellular) Algebras. Tech. Univ. München, Fak. f. Math. Report, TUM M9510(95).
- [10] R. Laue. *Construction of combinatorial objects, a tutorial*. Bayreuther Mathematische Schriften, 43: 53–96, 1993.
- [11] C.H. Li, *On isomorphisms of finite Cayley graphs - a survey*, Disc. Math. **256**(2002), 301-334.

- [12] M. Muzychuk, *Ádám's conjecture is true in the square-free case*, J. of Combin. Th. (A) **72**(1995), no. 1, 118-134.
- [13] M. Muzychuk, *On Ádám's conjecture for circulant graphs*, Discrete Math. **176**(1997), 285-298.
- [14] M. Muzychuk, *On the isomorphism problem for cyclic combinatorial objects*, Discrete Math. **197/198**(1999), 589-606.
- [15] M. Muzychuk, *A solution of isomorphism problem for circulant graphs*, Proc. of the London Math. Soc. 3 (88), 2004.
- [16] P.P. Pálffy, *Isomorphism problem for relational structures with a cyclic automorphism*, Europ. J. Comb. **8**(1987), 35-43.
- [17] K.T. Phelps, *Isomorphism problem for cyclic block designs*, Ann. Disc. Math., 34 (1987), pp. 385-392.
- [18] H. Wielandt, *Finite Permutation Groups*, Academic Press, 1964, Berlin.
- [19] H. Wielandt, *Permutation groups through invariant relations and invariant functions*, Lect. Notes., Dept. Math.m Ohio St. Univ, Colimbus, 1969.

NETANYA ACADEMIC COLLEGE, NETANYA, ISRAEL

E-mail address: `muzy@netanya.ac.il`